WEBINAIRE | 12 décembre 2025 | 11h00 - 11h30

www.france-innovation.fr

Hucency

Votre solution de sensibilisation à la cybersécurité

AU PROGRAMME

Les piliers de la solution

- **Cartographie des vulnérabilités humaines**
- **Sensibilisation aux cyberattaques**
- **Prévention des faux pas du quotidien**
- **Pilotage et accompagnement pour DSI et RSSI**
- Questions / réponses en direct

hucency
human centered cybersecurity

Anne-Claire Hénon
Chanel Business Developer

Margot Mayout
Chargée de partenariat

France Innovation

Explorez l'univers de

hucency
human centered cybersecurity

ex AvantdeCliquer .com
L'humain au cœur de la cybersécurité

Sensibilisez, formez et renforcez

vos équipes contre les cyberattaques

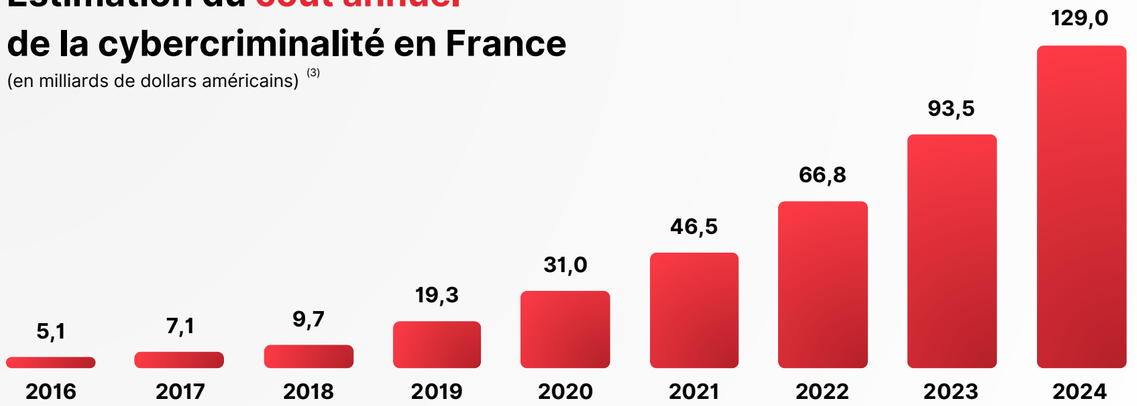
Conçu, créé et hébergé en France, depuis 2017

80 à 95%

des cyberattaques commencent par un email de phishing (1)

Estimation du coût annuel de la cybercriminalité en France

(en milliards de dollars américains) (3)

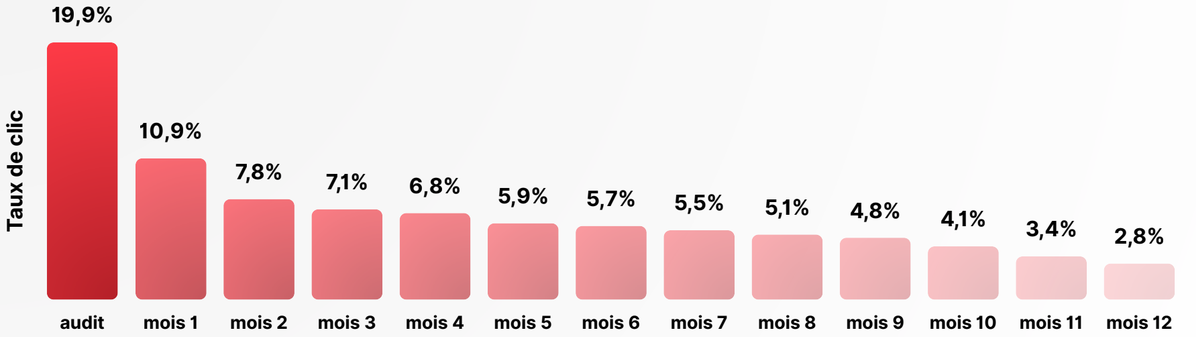


74%

de toutes les violations de données incluent l'élément humain (2)

Notre mission : Diviser par 10 le risque cyber dès la 1ère année

Moyenne réalisée sur 1 million d'utilisateurs tous secteurs confondus (privés ou publics)



Sources :
(1) https://www.securitymagazine.com/articles/99696-between-80-and-95-of-cyberattacks-begin-with-phishing
(2) https://secureframe.com/fr-fr/blog/data-breach-statistics
(3) Statista Technology Market Insights

hucency
human centered cybersecurity

Nos labels et récompenses

afaq ISO 27001 Sécurité de l'information AFNOR CERTIFICATION

MEMBRE

RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

CYBERMALVEILLANCE.GOUV.FR

Cas d'Or
de l'Association de l'Utilisateur au Dispositif de Sécurité

Lauréat de l'Innovation SANTEXPO
Transformation Digitale & Cybersécurité

Lauréat de l'Intelligence Économique
Trophées de l'Agroalimentaire

Finaliste du Prix de l'Innovation
du Salon des Maires et des Collectivités Locales

Bpifrance
Solution Pertinente pour Sensibiliser les Utilisateurs à la Cybersécurité

Mention Spéciale Expoprotection
Sûreté-Sécurité & Cyberprévention

Lauréat
Trophées Innovation Transformation par le Numérique

hucency
human centered cybersecurity

Let’s go!

offert

Avec notre Phishing Pentest offert, mettez votre organisation à l’épreuve !

Mesurez la vigilance de vos équipes et élaborez votre stratégie de sensibilisation avec une simulation réaliste, pensée pour évaluer les réflexes de vos collaborateurs face aux cybermenaces.

Notre conseil

Ne communiquez pas auprès de vos équipes avant cet état des lieux, afin de garantir des résultats authentiques.

Le principe

Pendant 5 jours ouvrés, notre algorithme envoie entre 1 et 4 emails de phishing différents à chaque utilisateur parmi une base de 50 à 100 modèles.

L’objectif

Observer la réaction naturelle de vos utilisateurs face à une menace et identifier les vulnérabilités humaines dans votre organisation.

À l’issue de cet état des lieux

Un expert vous restitue les résultats sous forme d’un rapport détaillé en visio ainsi que des recommandations personnalisées afin de définir votre stratégie de sensibilisation.

hucency
human centered cybersecurity

Menaces & prévention externes

Prévention interne

Pilotage

Comment **Hucency** répond aux différentes menaces ?

hucency
human centered cybersecurity

Menaces & prévention externes

Prévention interne

Pilotage

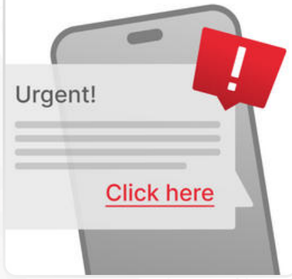
Le Phishing

Le Spear phishing

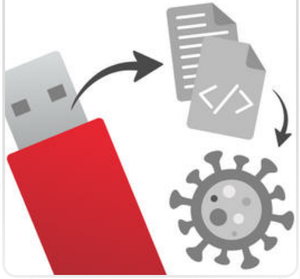
Les attaques spécifiques

Le Vishing

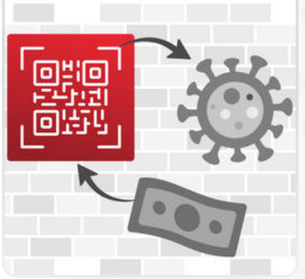
Le Smishing



L'USB dropping



Le Quishing



La sensibilisation ciblée et automatisée

hucency
human centered cybersecurity

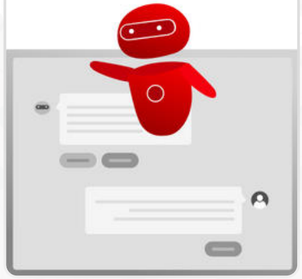
Menaces
& prévention
externes

Prévention interne

Pilotage

La plateforme eLearning

Le Chatbot



Le bouton “Alerte phishing”

Les écrans de veille, affiches, actualités

Thomas, votre RSSI virtuel

Real-Time Situational Awareness (RTSA)

hucency
human centered cybersecurity

Menaces & prévention externes

Prévention interne

Pilotage

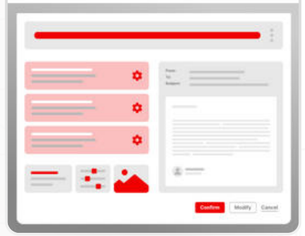
Tableau de suivi

Rapports

Surveillance dark web

Surveillance du nom de domaine

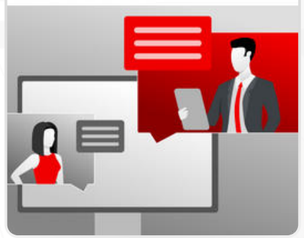
Outil de création de mise en situation personnalisée



Templates multilingue

Supervision multi-organisations

Accompagnement par des chargés de compte



Et maintenant ?

hucency
human centered cybersecurity

Menaces externes

hucency
human centered cybersecurity

Le Phishing

Le phishing est une technique de fraude en ligne où des escrocs se font passer pour des entreprises ou des institutions de confiance, comme des banques ou des sites de commerce, pour tromper vos collaborateurs.

Ils envoient souvent des emails, des messages ou des liens vers des sites web qui semblent légitimes, dans le but de récolter vos informations personnelles comme des mots de passe, des numéros de carte bancaire ou d'autres données sensibles.

Le Spear phishing

Le spear phishing est une forme d’hameçonnage plus ciblée.

Les escrocs personnalisent leurs messages pour un collaborateur précis ou une entreprise spécifique, en utilisant des informations qu'ils ont collectées pour paraître plus crédibles et vous tromper.

Les attaques spécifiques

Certaines situations nécessitent des approches plus ciblées.
Notre équipe de chargés de compte crée, à votre demande, des simulations d'attaques personnalisées, conçues en fonction du contexte, des habitudes ou des événements internes de votre organisation.

Que ce soit une campagne de communication interne, une période sensible ou un changement structurel, nous adaptons les scénarios pour coller au plus près de la réalité et tester efficacement la vigilance de vos collaborateurs.
Ces simulations sont pensées pour surprendre, faire réfléchir et ancrer durablement les bons réflexes.

Le Vishing

Le Vishing (ou hameçonnage vocal) est une forme de fraude où des escrocs utilisent des appels téléphoniques pour vous tromper.

Ils se font passer pour des représentants d'entreprises légitimes externes, comme des banques ou des services publics, ou bien internes, comme un Directeur Général, un responsable RH/informatique ou un collègue, etc., et tentent de vous convaincre de divulguer des informations personnelles, comme des numéros de carte bancaire ou des mots de passe.

Ces appels peuvent sembler urgents ou indispensables au bon fonctionnement de votre organisation pour vous inciter à agir rapidement sans réfléchir.

En savoir +

hucency
human centered cybersecurity

Le Vishing

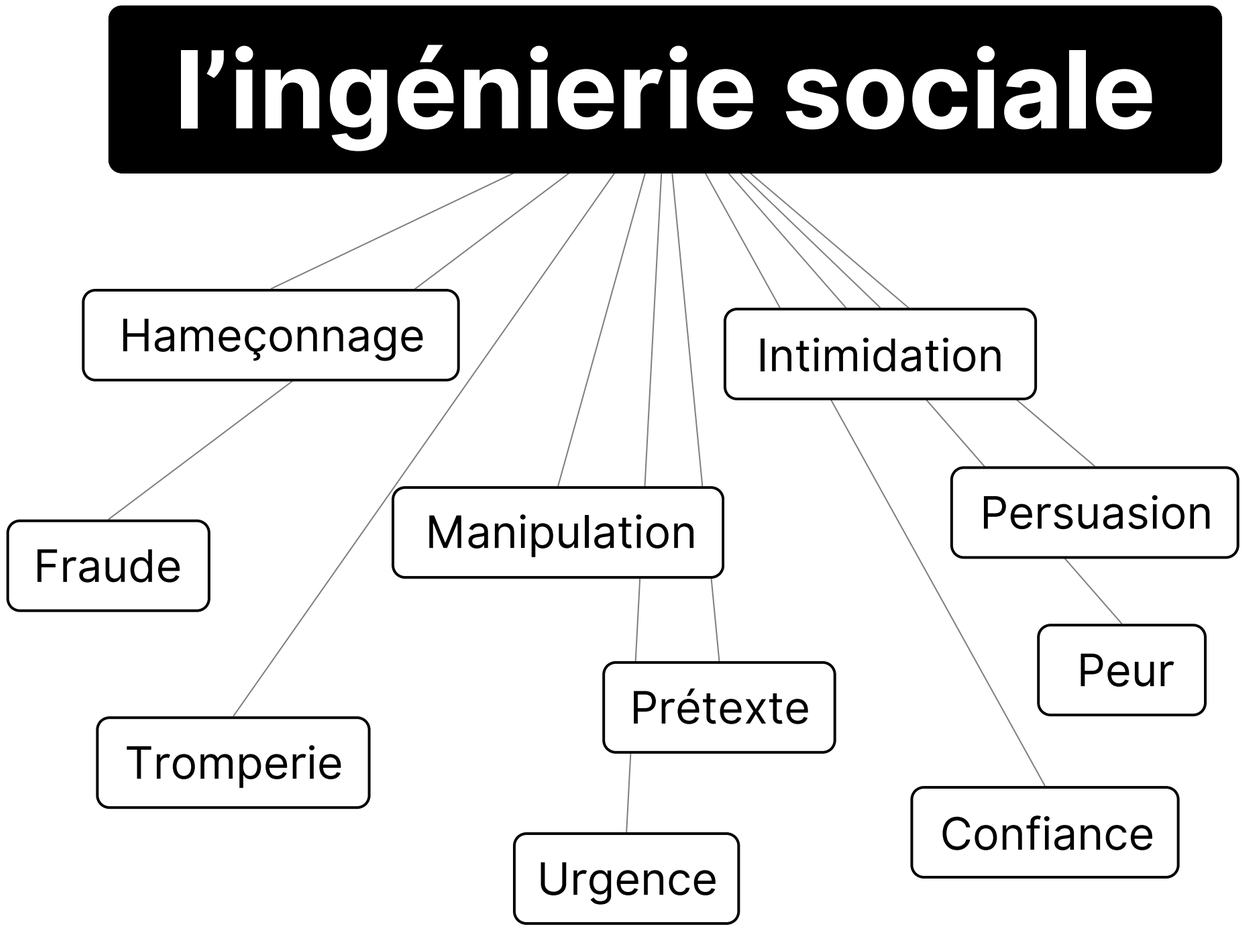
78%

d'escroqueries au faux conseiller bancaire
entre 2022 et 2023 (*)

1 500 victimes

sur une période de 6 mois (*)

Le pilier du **Vishing** est



* Source : Rapport d'activité 2023, Cybermalveillance.gouv.fr

hucency
human centered cybersecurity

Le Vishing (Réalisation de la mise en situation)

1 mois de prestation par campagne

Définition du ou des scénario(s)
et du nombre d'utilisateurs

Restitution des résultats
en visioconférence et livraison d'un rapport détaillé

hucency
human centered cybersecurity

Le Vishing (Des scénarios réalistes et adaptés)

Des scénarios adaptés au service concerné (RH, Achats, IT, Métiers, etc.)
avec un focus ou non sur des personnes à haut niveau de privilège ou des dirigeants.

1. Demander de mettre à jour un outil informatique en usurpant le helpdesk
2. Demander la réalisation d'une action d'un collaborateur ou d'un partenaire
3. Obtenir des renseignements sensibles sur l'organisation
4. Obtenir un code OTP en étant déjà en possession des *credentials* de l'utilisateur

Le Smishing

Le Smishing, ou hameçonnage par SMS, est une fraude en ligne où des escrocs vous envoient des messages texte frauduleux pour vous inciter à divulguer des informations personnelles.

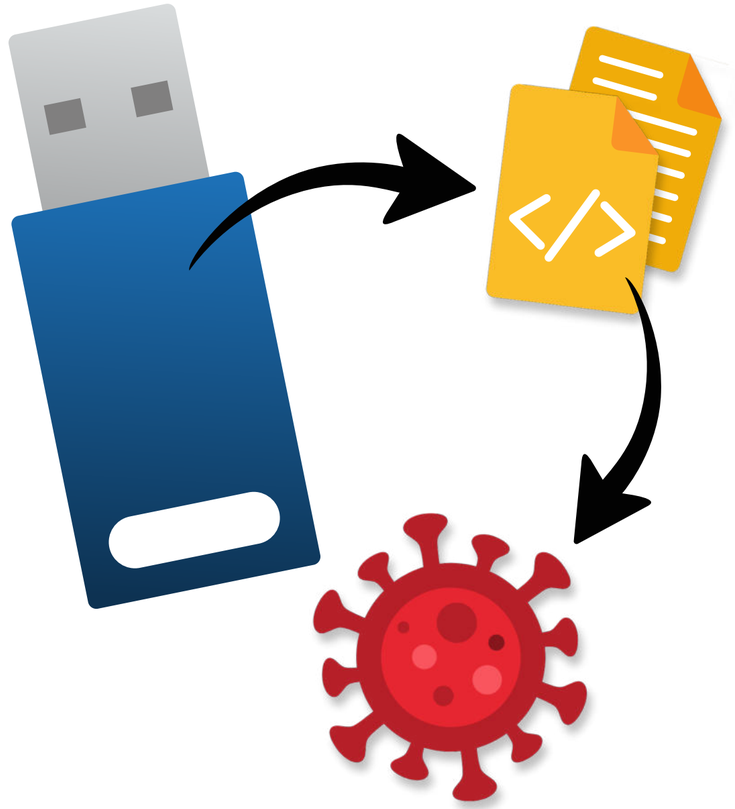
Ces messages semblent provenir de sources fiables, comme des banques ou des services de livraison, et contiennent souvent des liens vers des sites web falsifiés ou demandent des actions urgentes pour vous tromper et vous voler des données sensibles.

hucency
human centered cybersecurity

L’USB dropping

Les attaques par clé USB, appelées USB dropping ou USB phishing, consistent à laisser des clés USB infectées dans des lieux publics ou stratégiques, dans l'espoir que vous les récupériez et les branchiez à votre ordinateur.

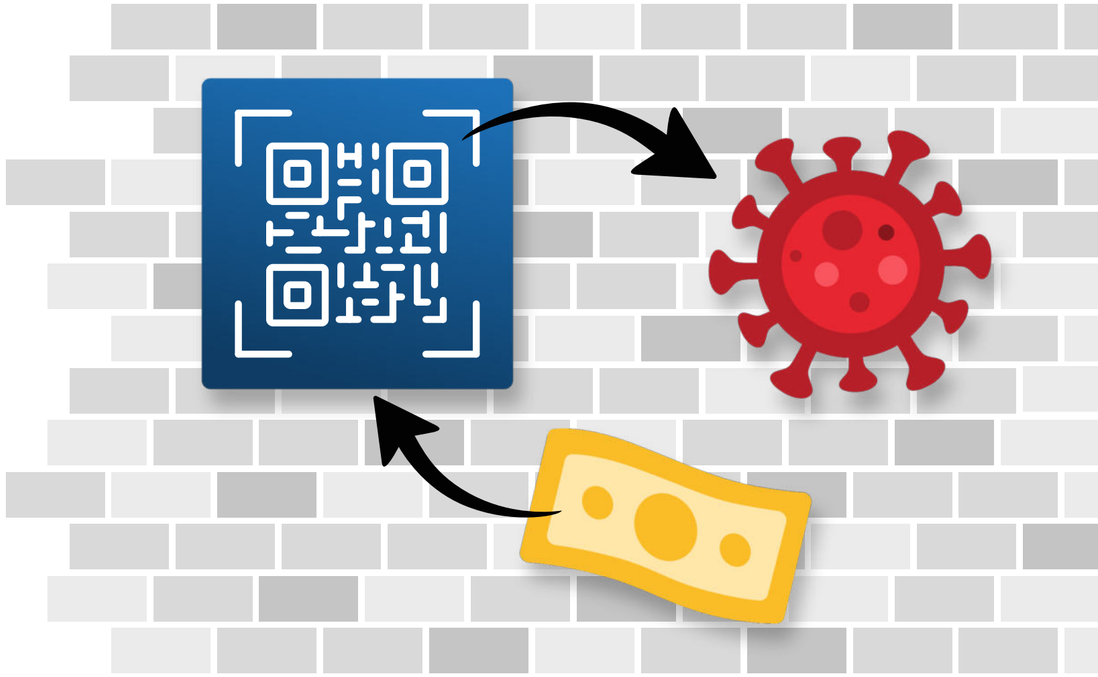
Une fois connectée, la clé peut installer des logiciels malveillants qui permettent aux attaquants d'accéder à vos données sensibles, de voler des informations ou de prendre le contrôle de votre ordinateur.



Le Quishing

Le Quishing est une forme d’hameçonnage utilisant des QR codes frauduleux pour vous rediriger vers des sites malveillants, vous voler des informations personnelles ou installer des logiciels malveillants.

Ces QR codes peuvent être placés sur des murs de bâtiments, des affiches, des documents ou des produits, vous incitant à les scanner et à vous laisser duper.



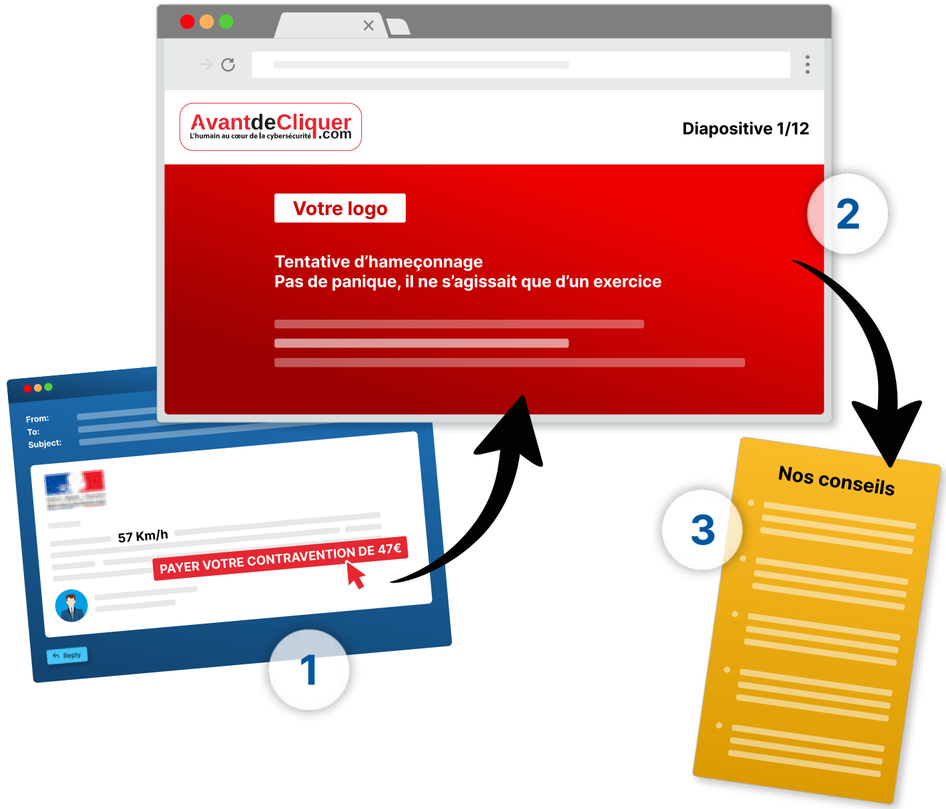
La sensibilisation ciblée et automatisée

Nous mettons en place des simulations d'attaques variées pour tester les réflexes des utilisateurs en situation réelle.

En confrontant les collaborateurs à des scénarios inspirés de véritables menaces, nous les aidons à reconnaître les pièges, à adopter les bons comportements et à renforcer durablement leur vigilance face aux cyberattaques.

Une approche concrète, efficace et pédagogique pour ancrer les bons réflexes.

Passons à quelques mises en situation...

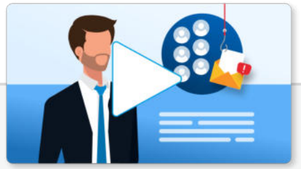


Prévention interne

hucency
human centered cybersecurity

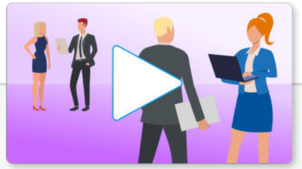
La plateforme eLearning

Notre programme de formation en ligne s’articule autour de trois formats de vidéos pédagogiques complémentaires, conçus pour adapter l’apprentissage aux besoins de chaque organisation et d’ancrer durablement les bons réflexes en cybersécurité.



Explications d’un expert

Un spécialiste expose les enjeux et bonnes pratiques, accompagnés de visuels et de textes dynamiques pour une compréhension optimale.



Mises en situation réalistes

Des scénarios joués par des employés pour plonger les collaborateurs dans des situations concrètes et renforcer leur capacité à réagir face aux cybermenaces.

Cours avec une formatrice

Une approche traditionnelle où une formatrice guide les apprenants à travers les concepts clés de la cybersécurité.

eLearning Nathan-Daesign

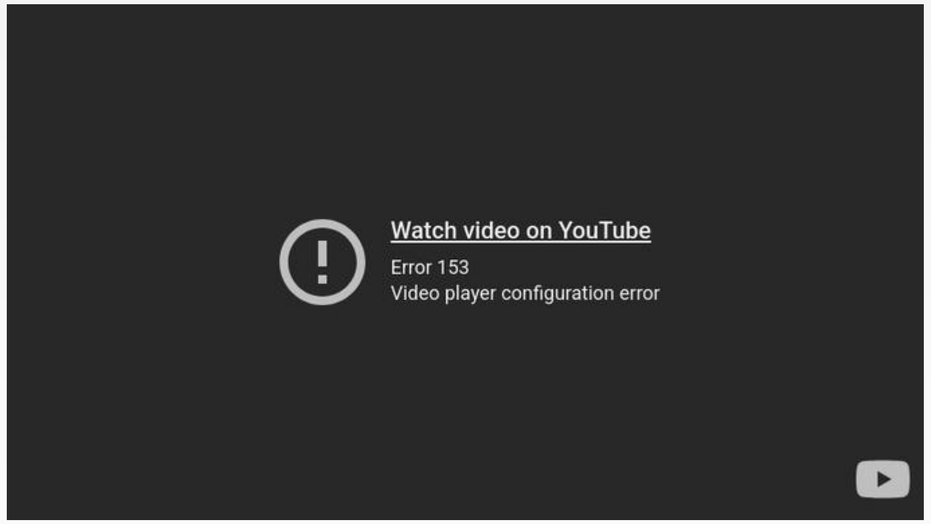
Un programme complémentaire “Cyber#365” ainsi que des modules e-Learning dispensés par notre partenaire Nathan Daesign.

* Un certificat sera délivré à la fin d’un suivi de parcours réussi. À quoi ça ressemble ?

Complément d’eLearning Nathan-Daesign

Le “bundle” Nathan Cyber#365

Cyber#365 est un programme de sensibilisation à la cybersécurité, clé en main, combinant e-learning, communication et campagnes interactives pour former les équipes tout au long de l’année.



En complément : modules RGPD, anticorruption, cyber et moi

Le parcours Daesign proposé pour Hucency est une solution e-learning clé en main pour sensibiliser efficacement les collaborateurs à la cybersécurité. Grâce à des modules immersifs, interactifs et scénarisés, il transforme la formation en véritable expérience engageante. Chaque séquence est conçue pour ancrer durablement les bons réflexes face aux cybermenaces. Une réponse concrète et impactante aux enjeux humains de la cybersécurité.

Consulter le document →

Nathan Compétences professionnelles

daesign

hucency human centered cybersecurity

L’attestation de suivi de formation eLearning

← Retour

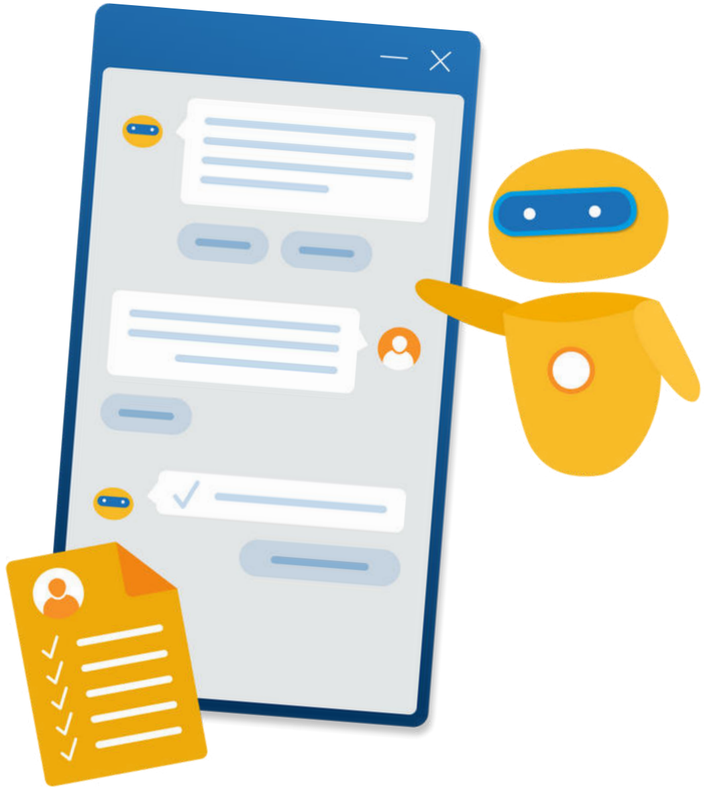
Le Chatbot

À tout moment, notre chatbot peut engager l'utilisateur en lui demandant s'il est disponible pour un court échange. Il interagit avec l'utilisateur en le questionnant sur les bonnes pratiques en cybersécurité.

À l'issue de l'échange, un rapport personnalisé lui est remis, lui permettant d'évaluer ses réflexes et d'identifier les points d'amélioration.

À quoi cela ressemble ?

Comment personnaliser votre scénario (à venir)

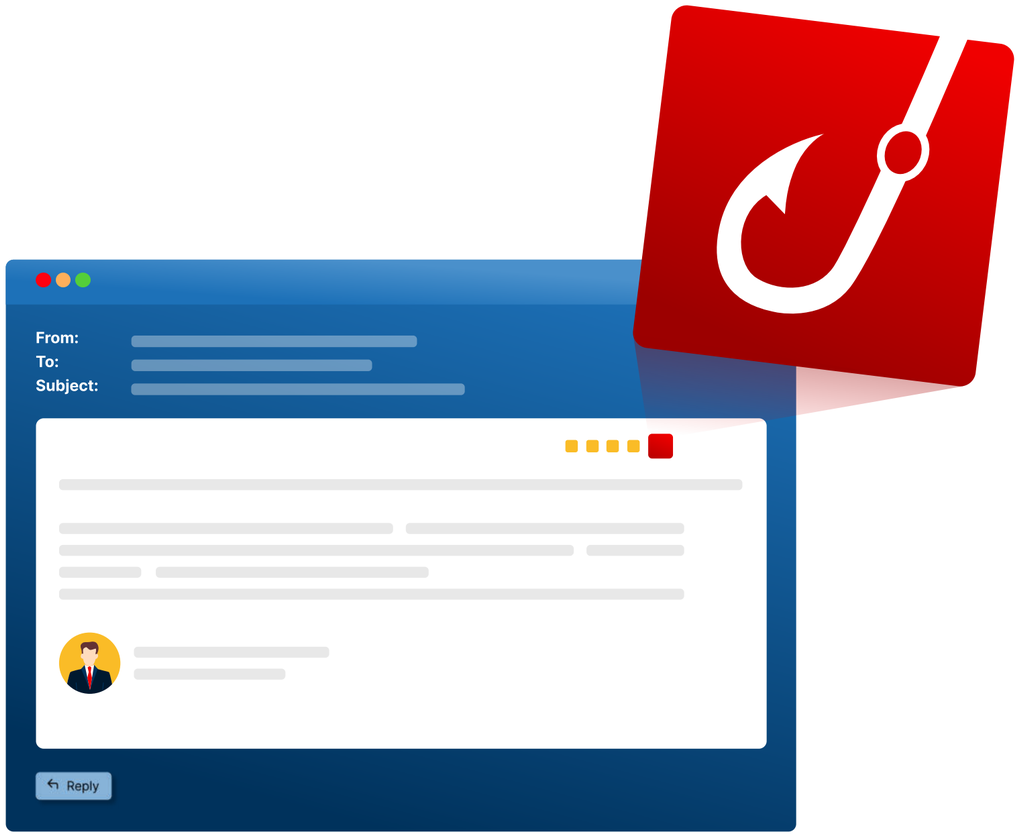


Le bouton “Alerte phishing”

Le Bouton Alerte Phishing (ou BAP) permet à vos collaborateurs de signaler instantanément une tentative de cyberattaque au DSI ou à l’équipe de sécurité.

En un seul clic, les menaces potentielles sont remontées pour une analyse rapide et une meilleure protection de l’organisation.

Je vous montre à quoi ça ressemble...



Les écrans de veille, affiches, actualités

Pour renforcer la sensibilisation au quotidien, nous mettons à disposition des affiches, des écrans de veille et de démarrage, ainsi qu'un accès aux actualités cybersécurité.

Ces supports visuels rappellent les bonnes pratiques et maintiennent l'attention de vos collaborateurs face aux menaces numériques.

Découvrir les visuels

Voir les actualités

hucency
human centered cybersecurity

L’affiche

Les écrans de veille →

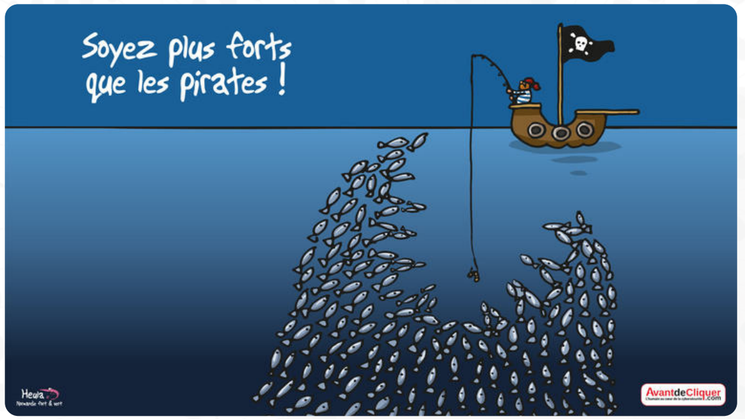
hucency human centered cybersecurity

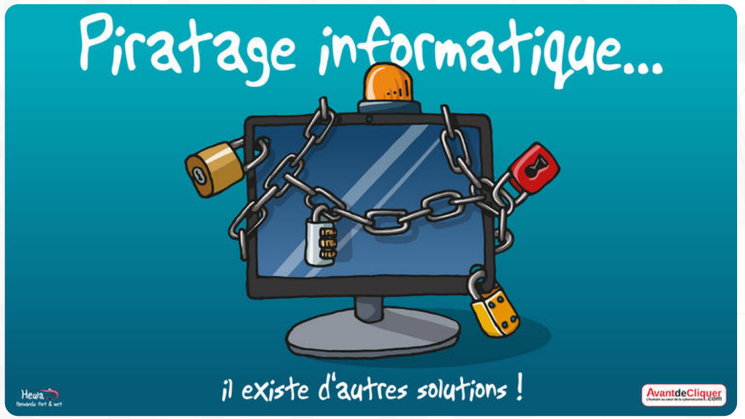
Les écrans de veille

Les fonds d’écran

hucency
human centered cybersecurity

Les fonds d’écran





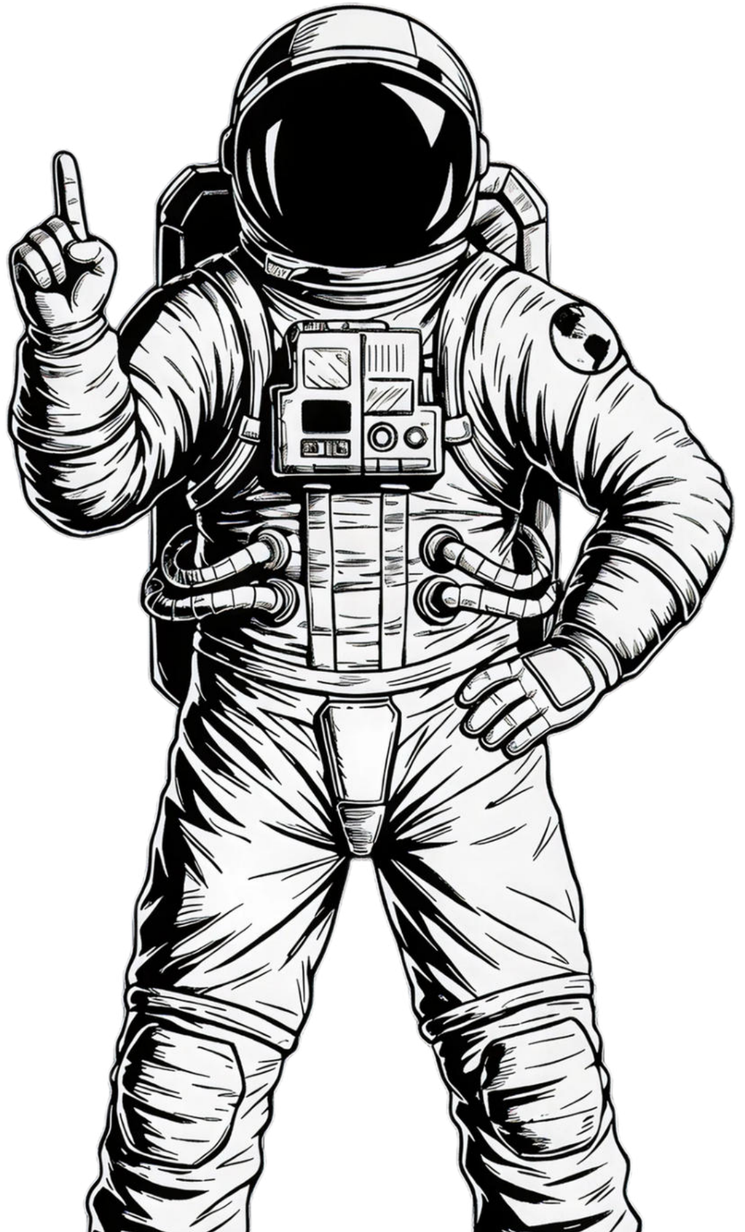
hucency
human centered cybersecurity

Thomas, votre RSSI virtuel

Thomas agit comme un Responsable Sécurité des Systèmes d'Information. Toujours disponible, il est directement intégré à l'environnement de vos collaborateurs.

Sous forme d'assistant intelligent, il répond à leurs questions, les guide face à une suspicion d'attaque et les oriente vers les bons réflexes à adopter.

Un soutien accessible à tout moment pour renforcer la réactivité et l'autonomie des collaborateurs face aux menaces.



hucency
human centered cybersecurity

Real-Time Situational Awareness (RTSA)

Le Real Time Situational Awareness (ou RTSA) permet d'intervenir immédiatement après une action à risque de l'utilisateur.

Qu'il s'agisse de libérer un email de quarantaine, de cliquer sur un lien suspect ou d'effectuer une action sensible, l'outil affiche une alerte contextualisée pour expliquer les risques potentiels et prévenir des conséquences.

Déployez dès à présent le plugin Windows et l'extension Chrome pour prévenir les risques et sensibiliser en temps réel vos utilisateurs.

Paramétrable par le Responsable informatique, il permet d'adapter les alertes aux besoins de l'organisation, renforçant ainsi la vigilance de chaque utilisateur au moment où cela compte le plus.

On vous fait une démo ?

Les bénéfices pour votre organisation

hucency
human centered cybersecurity

Real-Time Situational Awareness (RTSA)

Les bénéfices pour votre organisation

- **Réduction immédiate des comportements à risque**

Le RTSA intervient juste après une action sensible, ce qui permet de corriger les réflexes à chaud et de limiter les conséquences potentielles avant qu'il ne soit trop tard.

- **Sensibilisation contextuelle et personnalisée**

En affichant une alerte contextualisée et compréhensible, l'utilisateur est éduqué au moment même où il est exposé, ce qui favorise un apprentissage ancré et pertinent.

- **Paramétrage adapté à chaque environnement**

Grâce à un pilotage par le DSI/RSSI, les alertes et les cas d'usage sont adaptables à la réalité de chaque organisation, rendant la solution plus pertinente et opérationnelle.

- **Amélioration continue de la posture cyber**

En analysant les retours du RTSA, les responsables sécurité peuvent ajuster leurs actions de prévention et mieux cibler les besoins de formation ou d'accompagnement.

- **Déploiement facile et multiplateforme**

L'existence d'un plugin Windows et d'une extension Chrome permet une intégration rapide dans la majorité des environnements professionnels, sans infrastructure lourde.

Pilotage

hucency
human centered cybersecurity

Tableau de suivi

Notre tableau de bord interactif vous permet de suivre l’évolution de la sensibilisation de vos utilisateurs.

Il offre une vue d’ensemble des progrès, vous guide dans l’identification des axes d’amélioration et vous aide à ajuster les actions de formation pour une protection toujours plus efficace.

Accéder à la plateforme

Voir la vidéo de démo

Rapports

Chaque mois, les DSI, RSSI et managers reçoivent un rapport clair et structuré, incluant :

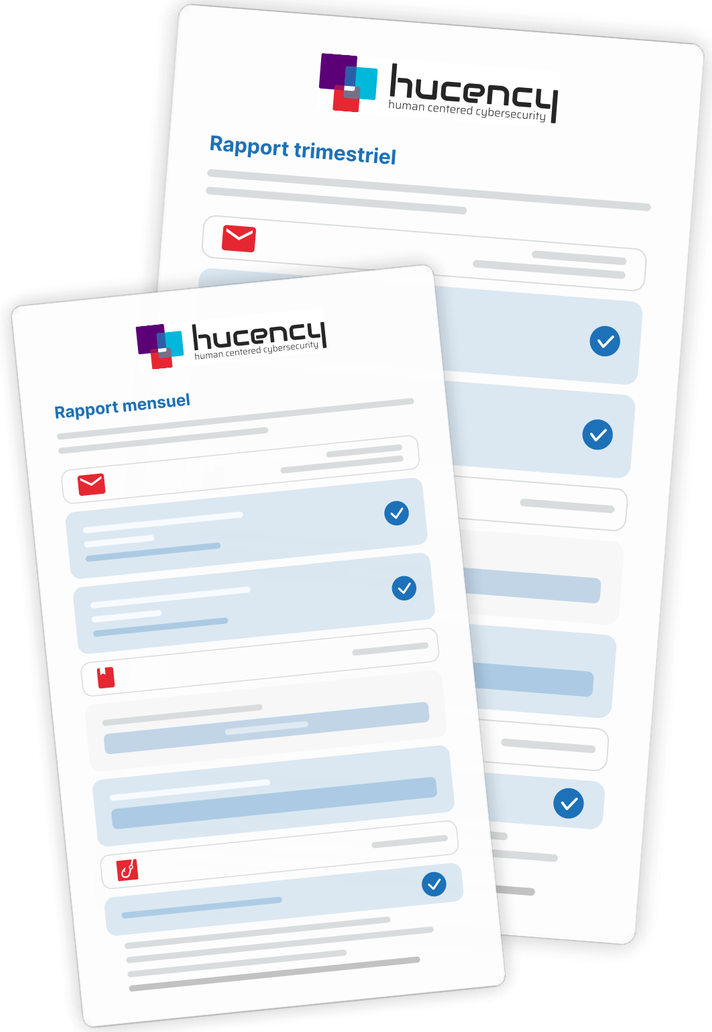
- un récapitulatif des mises en situation,
- un suivi des formations eLearning,
- et l'analyse de l'usage du bouton Alerte Phishing.

Un outil de pilotage essentiel pour mesurer l'engagement, ajuster les actions et renforcer la résilience de l'organisation.

Chaque trimestre, les utilisateurs reçoivent un bilan personnalisé de leur progression, favorisant implication et montée en compétence.

Voir un exemple

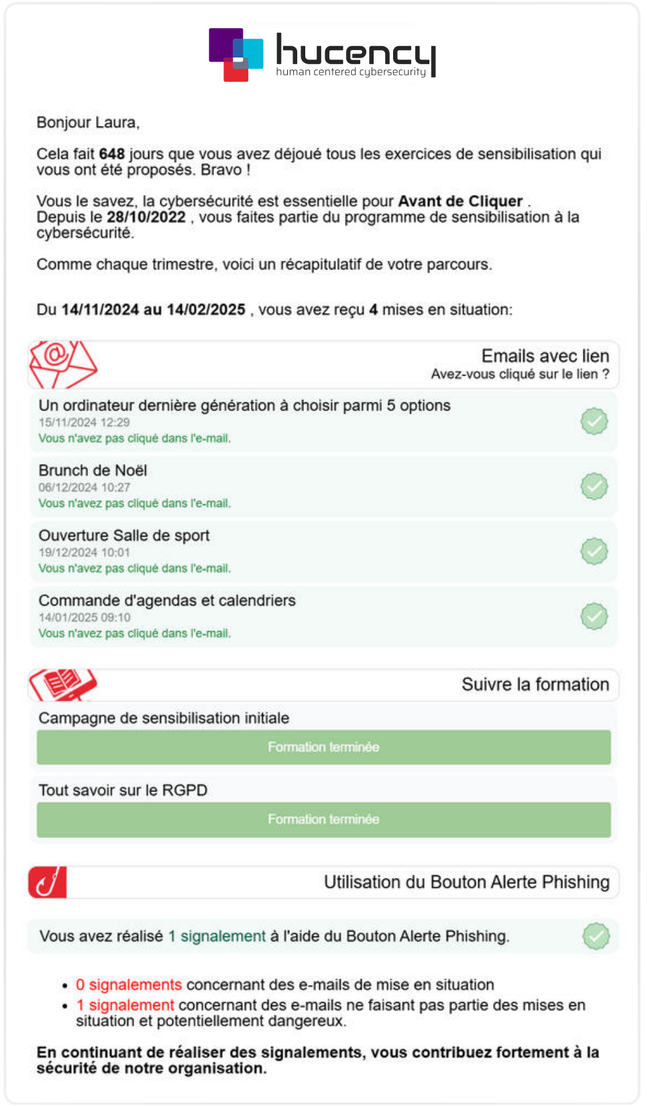
Ces rapports à forte valeur ajoutée mettent en lumière les progrès réalisés, détectent les vulnérabilités persistantes et intègrent des recommandations concrètes pour renforcer durablement la cybersécurité de votre organisation.



hucency
human centered cybersecurity

Rapports

(Aperçu d’un rapport trimestriel)



hucency
human centered cybersecurity

Bonjour Laura,

Cela fait **648** jours que vous avez déjoué tous les exercices de sensibilisation qui vous ont été proposés. Bravo !

Vous le savez, la cybersécurité est essentielle pour **Avant de Cliquer** .
Depuis le **28/10/2022** , vous faites partie du programme de sensibilisation à la cybersécurité.

Comme chaque trimestre, voici un récapitulatif de votre parcours.

Du **14/11/2024 au 14/02/2025** , vous avez reçu **4** mises en situation:

Emails avec lien
Avez-vous cliqué sur le lien ?

Un ordinateur dernière génération à choisir parmi 5 options
15/11/2024 12:29
Vous n'avez pas cliqué dans l'e-mail.

Brunch de Noël
06/12/2024 10:27
Vous n'avez pas cliqué dans l'e-mail.

Ouverture Salle de sport
19/12/2024 10:01
Vous n'avez pas cliqué dans l'e-mail.

Commande d'agendas et calendriers
14/01/2025 09:10
Vous n'avez pas cliqué dans l'e-mail.

Suivre la formation

Campagne de sensibilisation initiale
Formation terminée

Tout savoir sur le RGPD
Formation terminée

Utilisation du Bouton Alerte Phishing

Vous avez réalisé 1 signalement à l'aide du Bouton Alerte Phishing.

- 0 signalements concernant des e-mails de mise en situation
- 1 signalement concernant des e-mails ne faisant pas partie des mises en situation et potentiellement dangereux.

En continuant de réaliser des signalements, vous contribuez fortement à la sécurité de notre organisation.

hucency
human centered cybersecurity

Surveillance dark web

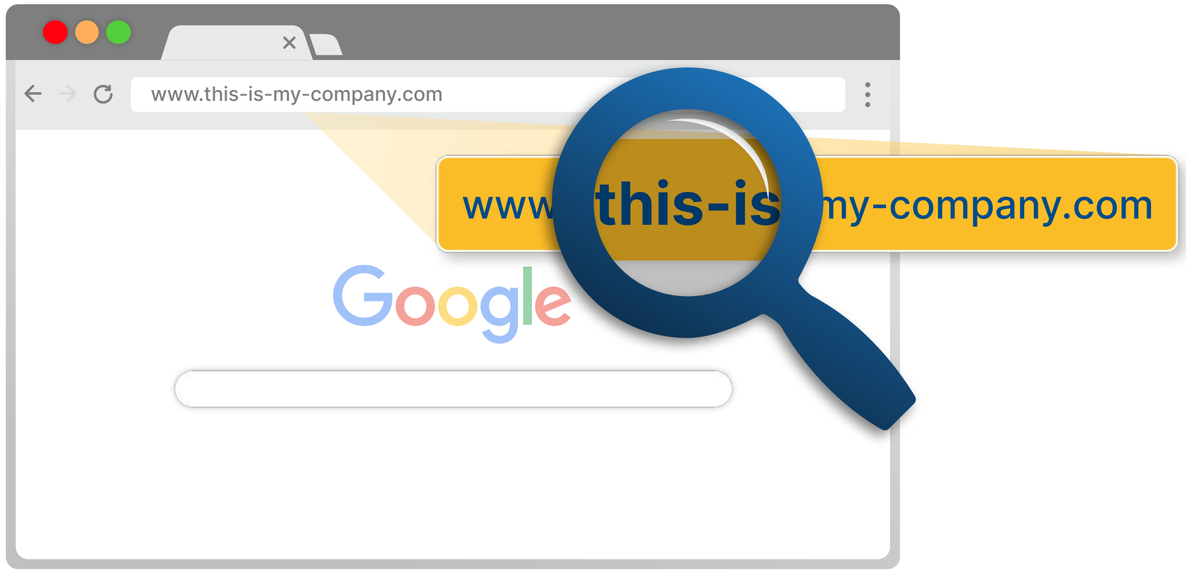
Notre service de surveillance web analyse en continu les bases de données compromises pour vérifier si les adresses email de votre organisation ont fuité sur le dark web.

Grâce à cette veille proactive, vous pouvez réagir rapidement et renforcer la sécurité de vos comptes avant qu'ils ne deviennent une porte d'entrée pour les cyberattaques.

Surveillance du nom de domaine

Nous surveillons en permanence votre nom de domaine pour détecter toute tentative de typosquatting ou d'usurpation. Cette veille permet d'identifier les domaines frauduleux imitant le vôtre, utilisés pour tromper vos collaborateurs, partenaires ou sous-traitants.

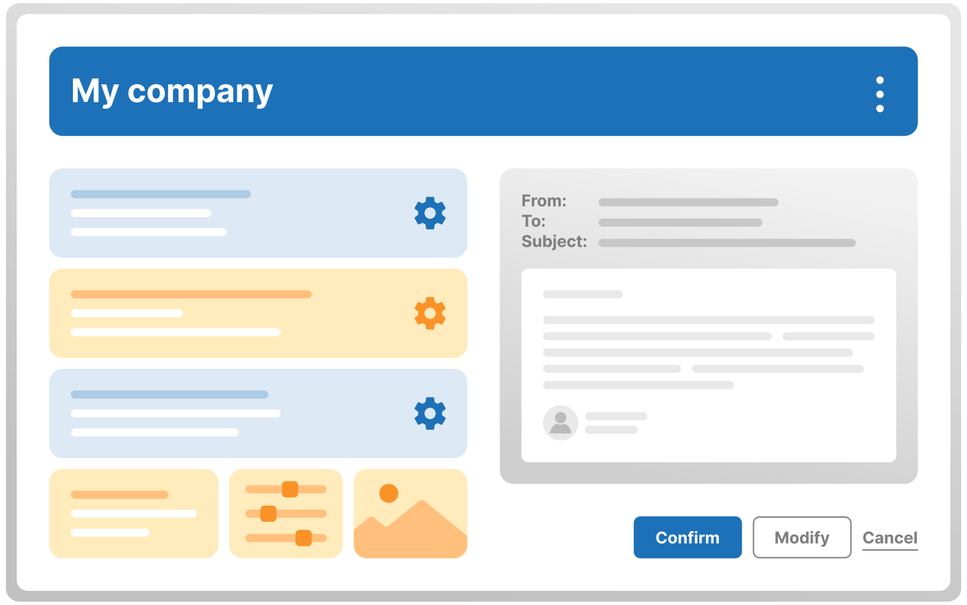
En anticipant ces menaces, vous protégez votre organisation contre les attaques par hameçonnage et usurpation d'identité.



Outil de création de mise en situation personnalisée

Notre outil de mise en situation personnalisée vous permet de concevoir et déployer vos propres fausses cyberattaques à destination de vos collaborateurs.

En adaptant les scénarios à votre contexte, vous maintenez la vigilance de vos équipes, identifiez les vulnérabilités et renforcez la sensibilisation de manière proactive.



hucency
human centered cybersecurity

Templates multilingue

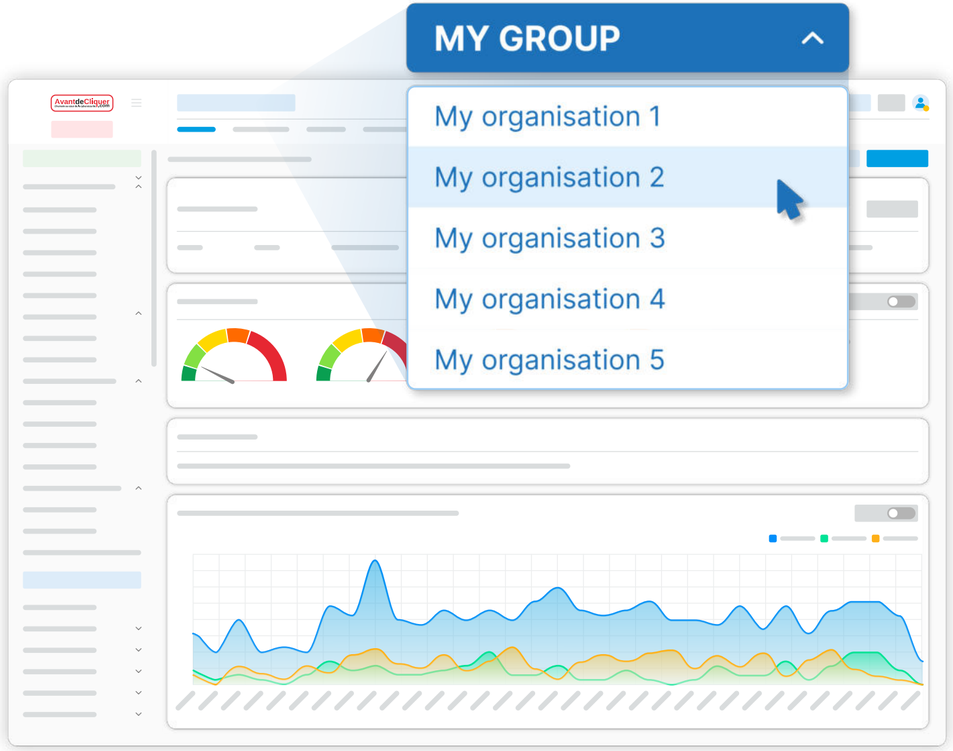
Avec plus d’un **millier de modèles** d’emails de phishing, nous proposons des simulations réalistes et variées pour tester la vigilance des collaborateurs.

Nos scénarios sont disponibles en une **trentaine de langues différentes**, garantissant une adaptation efficace aux contextes internationaux et aux spécificités culturelles de chaque organisation.

Supervision multi-organisations

Grâce à notre interface de suivi, gérez en toute simplicité plusieurs comptes au sein d'un même tableau de suivi.

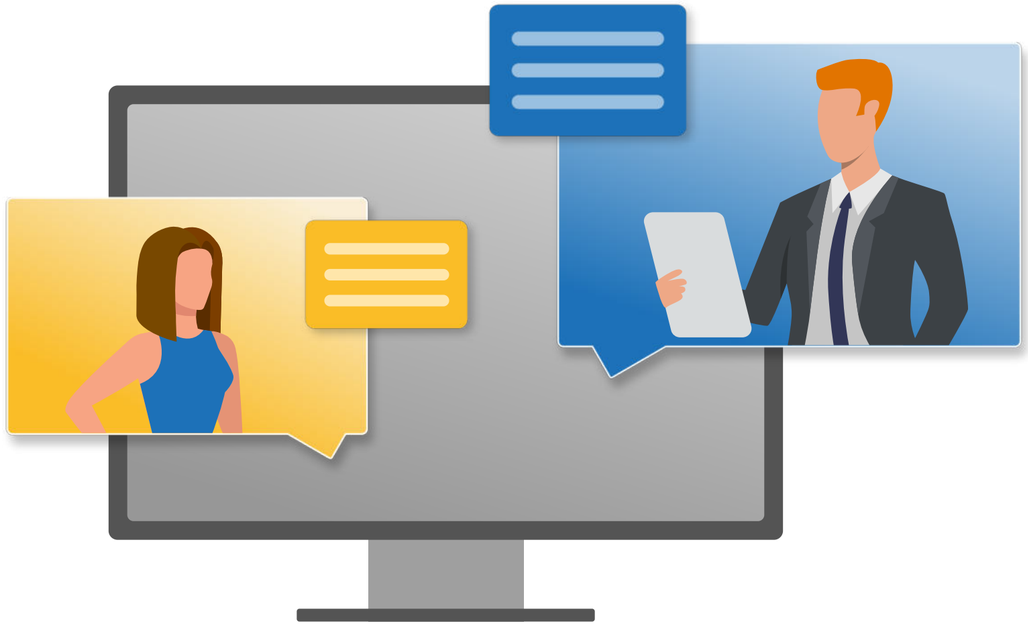
Conçue pour les groupes et organisations multi-entités, cette supervision permet d'avoir une vue d'ensemble claire des performances, de suivre l'évolution de la sensibilisation et d'adapter les actions de formation de manière centralisée.



Accompagnement par des chargés de compte

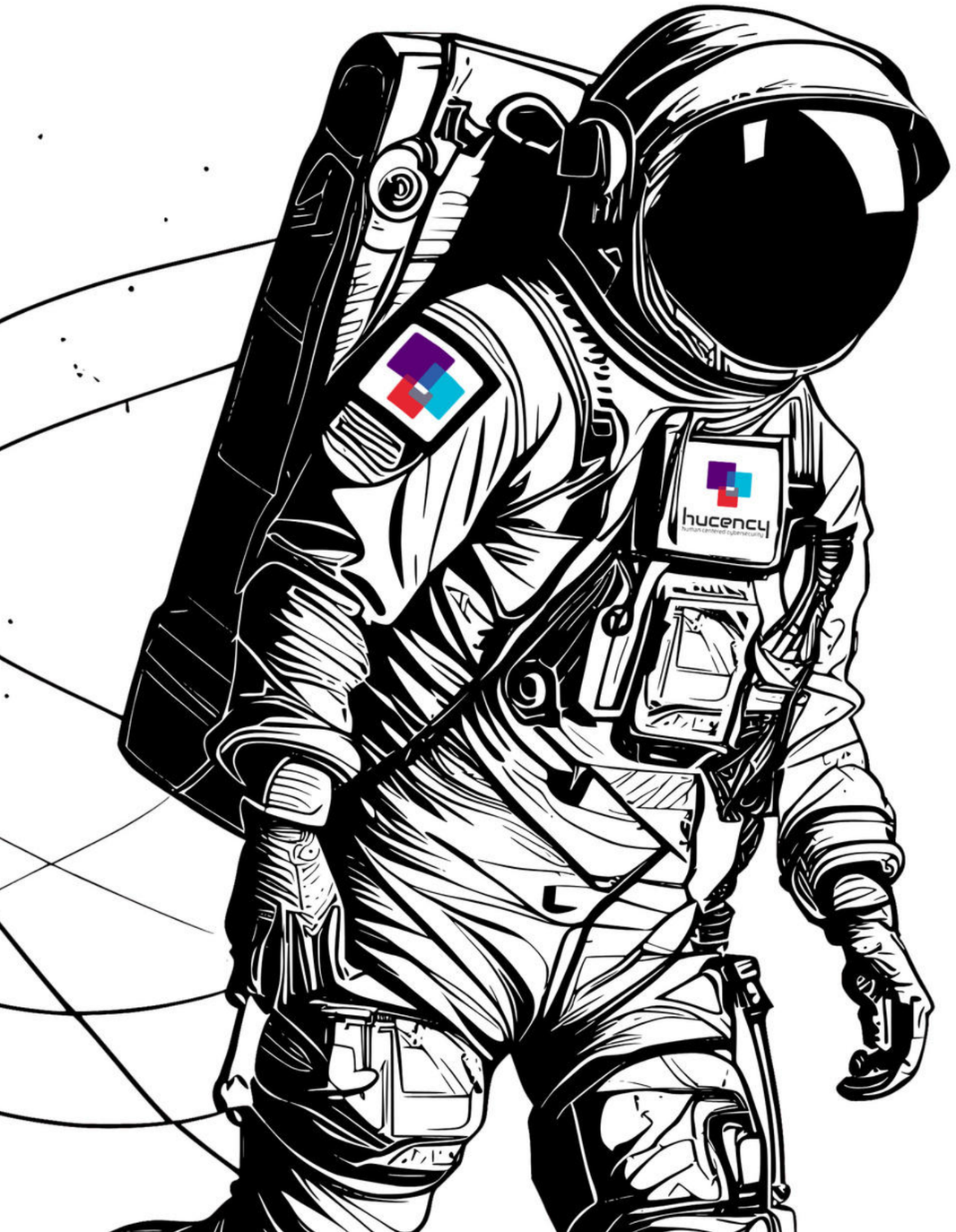
Nos chargés de compte vous accompagnent tout au long de votre parcours selon la fréquence la plus adaptée à votre organisation afin d'optimiser votre programme de sensibilisation.

De l'analyse des résultats à la mise en place d'actions correctives, ils assurent un suivi personnalisé, vous apportent des recommandations stratégiques et vous aident à maximiser l'efficacité de votre dispositif de cybersécurité.



Nouveauté à venir

Un peu de patience, nous faisons évoluer nos offres afin de rendre vos collaborateurs encore plus efficaces...



Il ne vous reste plus qu’à embarquer parmi le **million d’utilisateurs** déjà sensibilisés !

Les bénéfices pour votre organisation :

- **Lutter efficacement** contre les nouvelles typologies d’attaques
- **Sensibiliser les nouveaux arrivants** de votre organisation
- **Bénéficier des évolutions** constantes de la plateforme
- **Profiter d’un tarif préférentiel** bloqué sur 3 ans

hucency
human centered cybersecurity

Allo Houston ?!

On garde le contact ?

www.avantdecliquer.com

Suivez-nous sur

hucency
human centered cybersecurity

Anne-Claire **HENON**

Channel Business Developer

+33 2 21 81 41 78

anneclaire.henon@avantdecliquer.com

On prend RDV ?

Margot **MAYOUT**

Chargée de partenariat

+33 2 79 49 15 84

margot.mayout@avantdecliquer.com

On prend RDV ?


hucency
human centered cybersecurity